

(12)特許協力条約に基づいて公開された国際出願

(19)世界知的所有権機関
国際事務局



(43)国際公開日
2004年1月22日 (22.01.2004)

PCT

(10)国際公開番号
WO 2004/008684 A1

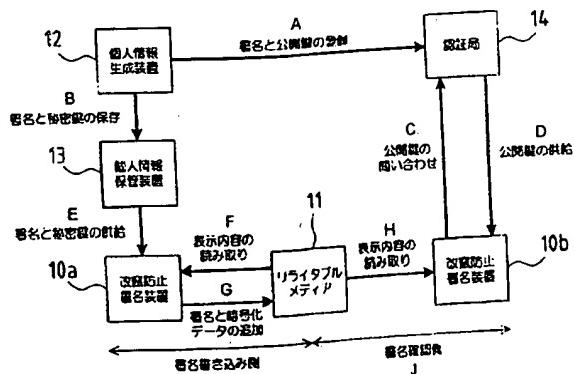
- (51)国際特許分類: H04L 9/32, G09C 1/00, G06T 7/00
- (21)国際出願番号: PCT/JP2003/008631
- (22)国際出願日: 2003年7月7日 (07.07.2003)
- (25)国際出願の言語: 日本語
- (26)国際公開の言語: 日本語
- (30)優先権データ: 特願2002-201444 2002年7月10日 (10.07.2002) JP
- (71)出願人(米国を除く全ての指定国について): シャープ株式会社 (SHARP KABUSHIKI KAISHA) [JP/JP]; 〒545-8522 大阪府 大阪市 阿倍野区長池町22番22号 Osaka (JP).
- (72)発明者; および
- (75)発明者/出願人(米国についてのみ): 吉村秀義
- (YOSHIMURA, Hideyoshi) [JP/JP]; 〒639-1007 奈良県 大和郡山市 南郡山町662、663 Nara (JP).
- (74)代理人: 倉内義朗 (KURAUCHI,Giro); 〒530-0047 大阪府 大阪市 北区西天満4丁目14番3号住友生命御堂筋ビル Osaka (JP).
- (81)指定国(国内): CN, US.
- (84)指定国(広域): ヨーロッパ特許(AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR).

添付公開書類:
— 国際調査報告書

2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイドスノート」を参照。

(54) Title: FALSE ALTERATION PREVENTION SIGNATURE METHOD

(54)発明の名称: 改竄防止署名方法



- 12..PERSONAL INFORMATION GENERATION DEVICE
- A..REGISTER SIGNATURE AND PUBLIC KEY
- 14..AUTHENTICATION AUTHORITY
- B..SAVE SIGNATURE AND PRIVATE KEY
- 13..PERSONAL INFORMATION STORAGE DEVICE
- C..MAKE INQUIRY ABOUT PUBLIC KEY
- D..SUPPLY PUBLIC KEY
- E..SUPPLY SIGNATURE AND PRIVATE KEY
- 10a ..FALSE ALTERATION PREVENTION SIGNATURE DEVICE
- F..READ DISPLAY CONTENTS
- G..ADD SIGNATURE AND ENCRYPTED DATA
- 11..RE-WRITABLE MEDIUM
- H..READ DISPLAY CONTENTS
- 10b ..FALSE ALTERATION PREVENTION SIGNATURE DEVICE
- I..SIGNATURE WRITING SIDE
- J..SIGNATURE CONFIRMATION SIDE

(57) Abstract: A false alteration prevention signature device comprises a feature extraction unit (33) that extracts a feature value representing the feature of image data according to an instruction from an authenticator who has authenticated display data; an encryption/decryption unit (35) that encrypts the feature value using an encryption key paired with an identifier to generate encrypted data, and decrypts the encrypted data into the feature value; a medium writing unit (34) that adds the identifier and the encrypted data to a re-writable medium; and a controller (37) that checks if the decrypted feature value matches the feature value extracted from image data generated by reading display data.

(57) 要約: 本改竄防止署名装置は、表示データを認証した認証者の指示により、画像データの特徴を表す特徴量を抽出する特徴抽出部33と、識別子と対になった暗号鍵を用いて特徴量を暗号化することにより暗号化データを生成し、かつ、暗号化データを特徴量に復号化する暗号化・復号化部35と、識別子と暗号化データとをリライタブルメディアに附加するメディア書き込み部34と、復号化された特徴量と表示データを読み込んで生成した画像データから抽出した特徴量との一致を判定するコントローラ37とを備えている。

WO 2004/008684 A1

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP03/08631

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl⁷ H04L9/32, G09C1/00, G06T7/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl⁷ H04L9/32, G09C1/00, G06T7/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
 Jitsuyo Shinan Koho 1922-1996 Jitsuyo Shinan Toroku Koho 1996-2003
 Kokai Jitsuyo Shinan Koho 1971-2003 Toroku Jitsuyo Shinan Koho 1994-2003

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2001-251295 A (Nippon Telegraph And Telephone Corp.), 14 September, 2001 (14.09.01), Full text; Figs. 1 to 12 (Family: none)	1-6
Y	JP 7-36383 A (Pitney Bowes Inc.), 07 February, 1995 (07.02.95), Full text; Figs. 1, 2 & DE 69332686 D & EP 599558 A & CA 2109553 A & US 5864622 A & US 6354494 B	1-6
Y	JP 2002-40936 A (NTT Advanced Technology Corp.), 08 February, 2002 (08.02.02), Full text; Figs. 1 to 5 (Family: none)	1-6

Further documents are listed in the continuation of Box C. See patent family annex.

* Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A" document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E" earlier document but published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O" document referring to an oral disclosure, use, exhibition or other means		
"P" document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search
07 October, 2003 (07.10.03)

Date of mailing of the international search report
21 October, 2003 (21.10.03)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.